BLOGS
Internet

Court Holds That Franchisor May Be Liable for Data Breach at Franchised Location

A federal court recently denied the motion of Wyndham Hotels & Resorts to dismiss a complaint brought by the Federal Trade Commission for unfair or deceptive acts or practices based on breaches of the property management computer system used by Wyndham and its franchisees. *FTC v. Wyndham Worldwide Corp.*, 2014 U.S. Dist. LEXIS 47622 (D.N.J. Apr. 7, 2014). The FTC alleged that franchisor Wyndham Hotels & Resorts, along with its affiliates, engaged in (1) deceptive practices by misrepresenting that it used "industry standard practices" and "commercially reasonable efforts" to secure the data it collected from guests, and (2) unfair practices by failing to protect customer data. Between 2008 and 2010, a criminal organization had hacked into the property management computer system multiple times—first through a franchisee's local computer network and then through an administrator account at one of the Wyndham entity's data centers. The hackers accessed credit card information from several hundred thousand guests of company-owned and franchised hotels, which allegedly resulted in $10.6 million in fraud losses. Wyndham moved to dismiss the complaint on the grounds that, among other things, the FTC did not sufficiently plead allegations to support its unfairness or deception claims, in part because the hotel businesses operated by franchisees are separate entities for which Wyndham is not legally responsible.

The court disagreed and rejected Wyndham's contention that "as a matter of law, it is necessarily a separate entity from Wyndham-branded hotels," such that each maintains its own computer networks and engages in separate data collection practices. The FTC alleged that Wyndham failed to provide reasonable security for the personal information collected by it and its franchisees, and the court found that allegation sufficient to withstand a motion to dismiss. The court also rejected Wyndham's argument that its privacy policy expressly disclaimed responsibility for the security of customer data collected by its franchisees. The court focused on other language in the same privacy policy that emphasized the "importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests" and stated that it "applies to residents of the United States, ***hotels of our Brands located in the United States***, and Loyalty Program activities." The court found that a reasonable customer might have understood the policy to cover data security practices at both company-owned and franchised hotels.

Related People

Maisa Frank

Partner

Washington, D.C.

202.295.2209

maisa.frank@lathropgpm.com